IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: Clough, et al.	)	Confirmation No: 8648
	)	
Serial No.: 10/004,173	)	Group Art Unit: 2625
	)	
Filed: October 9, 2001	)	Examiner: Milia, Mark R.
	)	
For: Method for Authenticating Mobile Printer Users	)	Atty. Docket No.: 10012945-1
	)	

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed November 22, 2006, responding to the final Office Action mailed September 22, 2006.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1-18 stand finally rejected. No claims have been allowed. The final rejections of claims 1-18 are appealed.

IV. Status of Amendments

This application was originally filed on October 9, 2001, with eighteen (18) claims. In a Response filed November 10, 2005, Applicant presented remarks without any claim amendments. In a Response filed February 27, 2006, Applicant presented remarks without any claim amendments. In a Response filed July 10, 2006, Applicant amended claims 6 and 10. The claims in the attached Claims Appendix (see below) reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a print server (Fig. 2, 112) for processing a print job (Fig. 3, 312) sent by a workstation (Fig. 2, 108). The print server (Fig. 2, 112) comprises a printer set-up module (Fig. 2, 114) to provide a print driver (Fig. 3, 304) for installation on the workstation (Fig. 2, 108). The print server (Fig. 2, 112) further comprises an authentication module (Fig. 2, 120) to supply an authentication code (Fig. 3, 302) to the workstation (Fig. 2, 108) and to review the print job (Fig. 3, 312) sent by the workstation (Fig. 2, 108) to determine validity of a copy of the authentication code (Fig. 3, 302A) attached to the print job (Fig. 3, 312). Applicant's specification, pages 5-7, lines 18-26.

Embodiments according to independent claim 6 describe a method of printing. The method comprises attaching a workstation (Fig. 2, 108) to a LAN (Fig. 2, 104) and downloading and installing a print driver (Fig. 3, 304) on the workstation (Fig. 2, 108). Applicant's specification, pages 5-7, lines 18-26; pages 8-9, lines 24-27; and blocks 502-508 of Fig. 5. The method further comprises downloading an authentication code (Fig. 3, 302) to the workstation (Fig. 2, 108) from a print server (Fig. 2, 112); sending a print job (Fig. 3, 312), containing the authentication code (Fig. 3, 302), from the workstation (Fig. 3, 108) to the print server (Fig. 2, 112); and verifying validity of the authentication code (Fig. 3, 303). Applicant's specification, pages 5-7, lines 18-26; page 10, lines 1-21; and blocks 506-514 of Fig. 5. Such a method also comprises sending the print job (Fig. 3, 312) from the print server (Fig.

2, 112) to a printer (Fig. 2, 110). Applicant's specification, pages 5-7, lines 18-26; page 10, lines 10-25; and blocks 512-516 of Fig. 5.

Embodiments according to independent claim 10 describe a method of authenticating a print job. The method comprises downloading and installing a print driver (Fig. 3, 304) on a workstation (Fig. 2, 108) and downloading an authentication code (Fig. 3, 302) to the workstation (Fig. 2, 108) from a print server (Fig. 2, 112). Applicant's specification, pages 5-7, lines 18-26; page 9, lines 4-27; and blocks 502-508 of Fig. 5. The method further comprises sending a print job (Fig. 3, 312), containing the authentication code (Fig. 3, 302), from the workstation (Fig. 2, 108) to the print server (Fig. 2, 112); verifying validity of the authentication code (Fig. 3, 302); and sending the print job (Fig. 3, 312) to a printer (Fig. 2, 110). Applicant's specification, pages 5-7, lines 18-26; page 10, lines 10-25; and blocks 510-516 of Fig. 5.

Embodiments according to independent claim 18 describe a print server. The print server (Fig. 2, 112) comprises a printer set-up module (Fig. 2, 114) to provide a print driver (Fig. 3, 304) for installation on a workstation (Fig. 2, 108) and an authentication module (Fig. 2, 120) to supply an authentication code (Fig. 3, 302) to the workstation (Fig. 2, 108) and to review a print job (Fig. 3, 312) processed by the print driver (Fig. 3, 304) and sent from the workstation (Fig. 2, 108) to determine validity of the authentication code (Fig. 3, 302) attached to the print job (Fig. 3, 312). Applicant's specification, pages 5-7, lines 18-26.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-18 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Barnard* (U.S. Patent Publication No. 2003/0005097) in view of *DeBry* (U.S. Patent No. 6,385,728).

VII. Arguments

The Appellant respectfully submits that Applicant's claims 1-18 are patentable under 35 U.S.C. §103. The Appellant respectfully requests that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

1. The *Barnard* Disclosure

Regarding *Barnard,* "[o]ne aspect of the invention concerns detecting a printing device connected on a network and requesting information from the detected printing device. The requested information is received from the printing device and a print queue is created for the printing device based on the received information." Para. 0011.

Also, *Barnard* discloses that "[n]etwork management device 20 then searches print drivers 60 for the appropriate print driver associated with the selected print queue. In step S1104, Network management device 20 configures the client workstation by sending and installing the appropriate print driver from print drivers 60 on workstation 12 via network 10. Once the print driver is installed on workstation 12, in step S1105 network management device 20 establishes a connection between

workstation 12 and print server 77, thereby allowing print jobs to be sent from workstation 12 to the selected print queue." Para. 0064.

2. The *DeBry* Disclosure

DeBry describes a system and method for guaranteeing authorization of a printer to retrieve a file directly from a file server. *See DeBry*, Patent Title. As is described by *DeBry*, a request to print a particular document is provided to a "document source 10," which stores files which may be available for printing. *See* col. 7, lines 15-16. This document source is separate from the printer. *See* FIGs. 1 and 3. Upon receiving the request, the document source creates a "will-call certificate" based upon the request and provides the certificate to the user. *See* col. 7, lines 16-19. The will-call certificate contains information that instructs the printer where to go to get the document. *See* col. 7, lines 20-25.

The user then takes the will-call request, builds a print request, and then sends the print request to the print server 30, which comprises the printer. *See* col. 7, lines 43-45; col. 6, lines 62-66; FIG. 3. The print server then goes to the document source, requests the document, and gives the will-call certificate to the document source. *See* col. 7, lines 50-53. The document source then verifies the identify of the printer and provides the requested document to the printer for printing. *See* col. 8, lines 32-36.

In one embodiment, the user is authenticated to ensure the user has the right to use the printer. *See* col. 9, lines 9-15. In this embodiment, the user sends a request for access of the printer to the printer along with the user's digital certificate. *See* col. 9, lines 16-18. The printer then sends a random message to the user, who encrypts the message with his private key and sends it back to the printer. *See* col. 9, lines 23-24. The printer decrypts the message with the user's public key and, if the message matches the original, the user is permitted to use the printer. *See* col. 9, lines 24-27.

As such, *DeBry* teaches that a "user requesting access would send, 401, such a request to the printer along with the user's digital certificate containing the user's public key. The printer may then send, 402, the public key and the user identification to a certificate authority 60 to authenticate the user's digital certificate." Col. 9, lines 16-20. This digital certificate is "from a trusted authority" which is not the print server that received the request.

3. Applicant's Claims 1-5

As provided in independent claim 1, Applicant claims:

> A print server, for processing a print job sent by a workstation, the print server comprising:
> a printer set-up module to provide a print driver for installation on the workstation; and
> ***an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job.***

(Emphasis added).

Applicant respectfully submits that claim 1 is allowable for at least the reason that the proposed combination of *Barnard* in view of *DeBry* does not disclose, teach, or suggest at least "an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job," as recited and emphasized above in claim 1.

The final Office Action of September 22, 2006 acknowledges that "Barnard does not disclose expressly an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job." Page 3. The Examiner alleges that *DeBry* discloses these features.

With regard to *DeBry*, it teaches that a "user requesting access would send, 401, such a request to the printer along with the user's digital certificate containing the user's public key. The printer may then send, 402, the public key and the user identification to a certificate authority 60 to authenticate the user's digital certificate." Col. 9, lines 16-20. This digital certificate is "from a trusted authority" which is not the print server that received the request. Accordingly, *DeBry* and *Barnard* fail to teach or suggest a print server having "an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job," since a user in neither the *DeBry* or *Barnard* systems receives an authentication code from a print server.

Accordingly, the proposed combination of *Barnard* in view of *DeBry* does not disclose all of the claimed features of claim 1. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination has not been made, and the rejection of claim 1 and claims 2-5 (which depend from claim 1) should be withdrawn.

4. Applicant's Claims 6-9

As provided in independent claim 6, Applicant claims:

> A method of printing, comprising:
> attaching a workstation to a LAN;
> downloading and installing a print driver on the workstation;
> ***downloading an authentication code to the workstation from a print server;***
> ***sending a print job, containing the authentication code, from the workstation to the print server;***
> ***verifying validity of the authentication code;*** and
> sending the print job from the print server to a printer.

(Emphasis added).

Applicant respectfully submits that claim 6 is allowable for at least the reason that the proposed combination of *Barnard* in view of *DeBry* does not disclose, teach, or suggest at least "downloading an authentication code to the workstation from a print server; sending a print job, containing the authentication code, from the workstation to the print server; [and] verifying validity of the authentication code," as recited and emphasized above in claim 6.

The final Office Action of September 22, 2006 acknowledges that "Barnard does not disclose expressly an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job." Page 3. The Examiner alleges that *DeBry* discloses these features.

With regard to *DeBry*, it teaches that a "user requesting access would send, 401, such a request to the printer along with the user's digital certificate containing the user's public key. The printer may then send, 402, the public key and the user identification to a certificate authority 60 to authenticate the user's digital certificate." Col. 9, lines 16-20. This digital certificate is "from a trusted authority" which is not the print server that received the request. Accordingly, *DeBry* and *Barnard* fail to teach or suggest at least "downloading an authentication code to the workstation from a print server; sending a print job, containing the authentication code, from the workstation to the print server; [and] verifying validity of the authentication code," since a user in neither the *DeBry* or *Barnard* systems receives an authentication code from a print server.

Accordingly, the proposed combination of *Barnard* in view of *DeBry* does not disclose all of the claimed features of claim 6. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination has not been

made, and the rejection of claim 6 and claims 7-9 (which depend from claim 6) should be withdrawn.

5. Applicant's Claims 10-12

As provided in independent claim 10, Applicant claims:

> A method of authenticating a print job, comprising:
> downloading and installing a print driver on a workstation;
> ***downloading an authentication code to the workstation from a print server;***
> ***sending a print job, containing the authentication code, from the workstation to the print server;***
> ***verifying validity of the authentication code;*** and
> sending the print job to a printer.

(Emphasis added).

Applicant respectfully submits that claim 10 is allowable for at least the reason that the proposed combination of *Barnard* in view of *DeBry* does not disclose, teach, or suggest at least "downloading an authentication code to the workstation; sending a print job, containing the authentication code, from the workstation to a print server; [and]verifying validity of the authentication code," as recited and emphasized above in claim 10.

The final Office Action of September 22, 2006 acknowledges that "Barnard does not disclose expressly an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job." Page 3. The Examiner alleges that *DeBry* discloses these features.

With regard to *DeBry*, it teaches that a "user requesting access would send, 401, such a request to the printer along with the user's digital certificate containing the user's public key. The printer may then send, 402, the public key and the user identification to a certificate authority 60 to authenticate the user's digital certificate."

Col. 9, lines 16-20. This digital certificate is "from a trusted authority" which is not the print server that received the request. Accordingly, *DeBry* and *Barnard* fail to teach or suggest at least "downloading an authentication code to the workstation; sending a print job, containing the authentication code, from the workstation to a print server; [and]verifying validity of the authentication code," since a user in neither the *DeBry* or *Barnard* systems receives an authentication code from a print server.

Accordingly, the proposed combination of *Barnard* in view of *DeBry* does not disclose all of the claimed features of claim 10. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination has not been made, and the rejection of claim 10 and claims 11-12 (which depend from claim 10) should be withdrawn.

6. Applicant's Claims 13-17

As provided in independent claim 13, Applicant claims:

> A processor-readable medium having processor-executable instructions thereon which, when executed by a computer, cause the computer to:
> download and install a print driver on a workstation;
> ***download and install an authentication code on the workstation from a print server;***
> ***send a print job, containing the authentication code, from the workstation to the print server;***
> ***verify validity of the authentication code using an authentication module on the print server;*** and
> send the print job from the print server to a printer.

(Emphasis added).

Applicant respectfully submits that claim 13 is allowable for at least the reason that the proposed combination of *Barnard* in view of *DeBry* does not disclose, teach, or suggest at least to "download and install an authentication code on the workstation from a print server; send a print job, containing the authentication code, from the

workstation to the print server; verify validity of the authentication code using an authentication module on the print server," as recited and emphasized above in claim 13.

The final Office Action of September 22, 2006 acknowledges that "Barnard does not disclose expressly an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job." Page 3. The Examiner alleges that *DeBry* discloses these features.

With regard to *DeBry*, it teaches that a "user requesting access would send, 401, such a request to the printer along with the user's digital certificate containing the user's public key. The printer may then send, 402, the public key and the user identification to a certificate authority 60 to authenticate the user's digital certificate." Col. 9, lines 16-20. This digital certificate is "from a trusted authority" which is not the print server that received the request. Accordingly, *DeBry* and *Barnard* fail to teach or suggest at least to "download and install an authentication code on the workstation from a print server; send a print job, containing the authentication code, from the workstation to the print server; verify validity of the authentication code using an authentication module on the print server," since a user in neither the *DeBry* or *Barnard* systems receives an authentication code from a print server.

Accordingly, the proposed combination of *Barnard* in view of *DeBry* does not disclose all of the claimed features of claim 13. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination has not been made, and the rejection of claim 13 and claims 14-17 (which depend from claim 13) should be withdrawn.

7. Applicant's Claim 18

As provided in independent claim 18, Applicant claims:

> A print server, comprising:
> a printer set-up module to provide a print driver for installation on a workstation; and
> ***an authentication module to supply an authentication code to the workstation, and to review a print job processed by the print driver and sent from the workstation to determine validity of the authentication code attached to the print job.***

(Emphasis added).

Applicant respectfully submits that claim 18 is allowable for at least the reason that the proposed combination of *Barnard* in view of *DeBry* does not disclose, teach, or suggest at least "an authentication module to supply an authentication code to the workstation, and to review a print job processed by the print driver and sent from the workstation to determine validity of the authentication code attached to the print job," as recited and emphasized above in claim 18.

The final Office Action of September 22, 2006 acknowledges that "Barnard does not disclose expressly an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job." Page 3. The Examiner alleges that *DeBry* discloses these features.

With regard to *DeBry*, it teaches that a "user requesting access would send, 401, such a request to the printer along with the user's digital certificate containing the user's public key. The printer may then send, 402, the public key and the user identification to a certificate authority 60 to authenticate the user's digital certificate." Col. 9, lines 16-20. This digital certificate is "from a trusted authority" which is not the print server that received the request. Accordingly, *DeBry* and *Barnard* fail to teach or suggest at least a print server having "an authentication module to supply an

authentication code to the workstation, and to review a print job processed by the print driver and sent from the workstation to determine validity of the authentication code attached to the print job," since a user in neither the *DeBry* or *Barnard* systems receives an authentication code from a print server.

Accordingly, the proposed combination of *Barnard* in view of *DeBry* does not disclose all of the claimed features of claim 18. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination has not been made, and the rejection of claim 18 should be withdrawn.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: 

Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A print server, for processing a print job sent by a workstation, the print server comprising:

a printer set-up module to provide a print driver for installation on the workstation; and

an authentication module to supply an authentication code to the workstation, and to review the print job sent by the workstation to determine validity of a copy of the authentication code attached to the print job.

2. The print server of claim 1, additionally comprising:

a software library to contain the print driver and at least one additional print driver.

3. The print server of claim 1, additionally comprising:

a webpage interface to gather information from the workstation to indicate a preferred print driver to be sent to the workstation.

4. The print server of claim 1, additionally comprising:

a web page to present a questionnaire to a user of the workstation.

5. The print server of claim 1, additionally comprising:

a MAC address, transferred from the workstation to the print server, to aid in the authentication of the workstation.

6. A method of printing, comprising:

attaching a workstation to a LAN;

downloading and installing a print driver on the workstation;

downloading an authentication code to the workstation from a print server;

sending a print job, containing the authentication code, from the workstation to the print server;

verifying validity of the authentication code; and

sending the print job from the print server to a printer.

7. The method of claim 6, additionally comprising:

obtaining information about the workstation; and

using the information to select the print driver from a library.

8. The method of claim 6, additionally comprising:

using a MAC address to assist in authenticating print jobs from the workstation.

9. The method of claim 6, additionally comprising:

using a webpage to present a questionnaire to a user of the workstation.

10. A method of authenticating a print job, comprising:

downloading and installing a print driver on a workstation;

downloading an authentication code to the workstation from a print server;

sending a print job, containing the authentication code, from the workstation to the print server;

verifying validity of the authentication code; and

sending the print job to a printer.

11. The method of claim 10, additionally comprising:

gathering information from the workstation to indicate a preferred print driver to be sent to the workstation.

12. The method of claim 10, additionally comprising:

using a MAC address to aid in authenticating that the print job was sent from an authorized location.

13. A processor-readable medium having processor-executable instructions thereon which, when executed by a computer, cause the computer to:

download and install a print driver on a workstation;

download and install an authentication code on the workstation;

send a print job, containing the authentication code, from the workstation to a print server;

verify validity of the authentication code using an authentication module on the print server; and

send the print job from the print server to a printer.

14. The processor-readable media of claim 13, having further instructions which cause the processors to:

gather information from the workstation to indicate a preferred print driver to be sent to the workstation.

15. The processor-readable media of claim 13, having further instructions which cause the processors to:

obtain information about the workstation; and

use the information to select the print driver from a library.

16. The processor-readable media of claim 13, having further instructions which cause the processors to:

use a MAC address aid in recognizing a location of the workstation.

17. The processor-readable media of claim 13, having further instructions which cause the processors to:

obtain information about the workstation from fields sent by a browser on the workstation.

18. A print server, comprising:

a printer set-up module to provide a print driver for installation on a workstation; and

an authentication module to supply an authentication code to the workstation, and to review a print job processed by the print driver and sent from the workstation to determine validity of the authentication code attached to the print job.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal.

Therefore, no such proceedings are identified in this Appendix.